

CLAIMS

1. A telecommunications system arranged for providing Single Sign-On services for a user (3) roaming in a packet radio network (CN-1, SN-1; CN-2, SN-2) of a Multinational Mobile Network Operator (MN-MNO) that includes a federation of National Network Operators (N-MNO-A; N-MNO-B), one of these National Network Operators (N-MNO-A) holding the user's subscription, the telecommunications system comprising:
- 5 - a visited Gateway GPRS Support Node (V-GGSN) (14) assigned for the user at a visited packet radio network (CN-1) wherein the user is roaming, and responsible for sending user's identifiers relevant for a first user's authentication toward the user's home network; and
 - 10 - a home Authentication, Authorization and Accounting (H-AAA) server (23) in the user's home service network (SN-2), responsible for maintaining a master session for the user with said user's identifiers;
 - 15 and **characterised in that** it further comprises:
 - 20 - a visited Authentication, Authorization and Accounting (V-AAA) server (13) in the visited network (SN-1), acting as a proxy between the V-GGSN (14) and the H-AAA (23), and binding an H-AAA address with said user's identifiers; and
 - 25 - a global Single Sign-On Front End (G-SSO-FE) infrastructure (33) intended to act as a single entry point for Single Sign-On service in the Multinational Mobile Network Operator federation.

2. The telecommunications system of claim 1, further comprising a Global Directory (31) of the Multinational Mobile Network Operator (MN-MNO) federation cooperating with the visited Authentication, Authorization and Accounting (V-AAA) server (13) in the visited network (SN-1) wherein the user is roaming to locate the home Authentication, Authorization and Accounting (H-AAA) server (23) in the user's home service network (SN-2).
3. The telecommunications system of claim 2, wherein the Global Directory (31) is an entity arranged for storing an association between user's identifiers relevant for user's authentication and an address of a corresponding home Authentication, Authorization and Accounting (H-AAA) server (23).
4. The telecommunications system of claim 1, wherein the visited Authentication, Authorization and Accounting (V-AAA) server (13) in the visited network (SN-1) wherein the user is roaming, keeps a binding of a home Authentication, Authorization and Accounting (H-AAA) server (23) address and user's identifiers within a Local Dynamic Routing Database (LDR DB) (11).
5. The telecommunications system of claim 4, wherein said user's identifiers comprise a user directory number and an IP address assigned to the user (UE) (3).
6. The telecommunications system of claim 1, wherein the home Authentication, Authorization and Accounting (H-AAA) server (23) in the user's home service network (SN-2) maintains a master session for the user in cooperation with a Single Sign-On Session Database (SSO Session DB) (21) responsible for storing session related information comprising a user directory number, an IP address assigned to the user, an indicator of a selected authentication mechanism, and a timestamp.

7. The telecommunications system of claim 1, further comprising a number of Service Providers (2) that have signed service agreements with the Multinational Mobile Network Operator (MN-MNO) federation for offering Single Sign-On services to users that are subscribers of any National Network Operator (N-MNO-A; N-MNO-B) included in the federation, each Service Provider (2) comprising:

- means for redirecting a user to a global Single Sign-On Front End (G-SSO-FE) infrastructure (33) as entry point in the federation;

- means for receiving a token from the user, the token being either an authentication assertion, or a reference thereof along with an indication of where such assertion was generated;

- means for retrieving an assertion from a site where the assertion was generated; and

- means for checking that such site is trusted.

8. The telecommunications system of claim 7, wherein each particular Service Provider (2) may have a different global Single Sign-On Front End (G-SSO-FE) (33) for acting as entry point in the federation.

9. The telecommunications system of claim 8, wherein each particular Service Provider (2) further comprises means for changing from one global Single Sign-On Front End (G-SSO-FE) (33) to one another within the federation for acting as entry point in said federation.

10. A method for providing Single Sign-On services through a number of Service Providers (2) having service agreements with a Multinational Mobile Network Operator (MN-MNO) for a user (3) roaming in a packet radio

network (CN-1, SN-1; CN-2, SN-2) of said Multinational Mobile Network Operator (MN-MNO) that includes a federation of National Network Operators (N-MNO-A; N-MNO-B), one of these National Network Operators (N-MNO-A) holding a user's subscription, the method comprising the steps of:

(a) performing a first authentication of a user roaming in a visited packet radio network (CN-1, SN-1) toward the user's home service network (SN-2); and

(b) creating a master session at the user's home service network (SN-2) with Single Sign-On related data;

the method **characterised by** including the steps of:

(c) redirecting a user accessing a Service Provider (2) that has a service agreement with the Multinational Mobile Network Operator (MN-MNO) toward the user's home network (N-MNO-A) via a global Single Sign-On Front End (G-SSO-FE) infrastructure (33) acting as entry point in the federation for obtaining a Single Sign-On authentication assertion; and

(d) receiving a Single Sign-On authentication assertion either from the user or from an entity where such assertion was generated.

11. The method of claim 10, wherein the step b) of creating a master session at the user's home service network (SN-2) with Single Sign-On related data is further **characterised by** including the steps of:

- storing at a Single Sign-On Session Database (21) Single Sign-On related data comprising a session identifier, a session status, a user directory number, an IP address assigned to the user, an

indicator of a selected authentication mechanism,
and a timestamp of the authentication event; and

- binding at a user's visited service network (SN-1)
an address of an entity handling the master session
for such user at the user's home service network
(SN-2), and a set of user's identifiers that
includes at least a user directory number, and an IP
address assigned to the user (3).

12. The method of claim 10, wherein the step a) of
performing a first authentication of a user roaming in
a visited packet radio network (CN-1) includes a step
of assigning a visited Gateway GPRS Support Node (14)
for the user at the visited packet radio network.

13. The method of claim 12, wherein the step of assigning a
visited Gateway GPRS Support Node includes a step of
sending user's identifiers relevant for a first user's
authentication from said visited Gateway GPRS Support
Node (14) toward a home Authentication, Authorization
and Accounting server (23) in the user's home service
network (SN-2) for maintaining a user's master session.

14. The method of claim 13, wherein the step of sending
user's identifiers includes a step of interposing a
visited Authentication, Authorization and Accounting
server (13) in the visited network (SN-1), acting as a
proxy between said visited Gateway GPRS Support Node
(14) and the home Authentication, Authorization and
Accounting server (23) in user's home network (SN-2).

15. The method of claim 10, wherein the step c) of
redirecting a user toward the user's home network (N-
MNO-A) via a global Single Sign-On Front End (G-SSO-FE)
infrastructure (33) comprises the steps of:

(c1) determining a visited network (N-MNO-B) which assigned the current IP address to the user when accessing the federation network; and

5 (c2) obtaining from the visited network (N-MNO-B) an address of an entity handling a user's master session in the user's home service network (SN-2).

16. The method of claim 15, wherein the step c2) of obtaining an address of an entity handling the master session for such user includes a step of redirecting
10 (S-54, S-55) the user toward the currently visited network (N-MNO-B).

17. The method of claim 15, wherein the step c2) of obtaining an address of an entity handling the master session for such user includes a step of requesting
15 such address from the global Single Sign-On Front End (33) toward the visited network (N-MNO-B) by using a Back-End protocol (S-90).

18. The method of claim 15, wherein the step c1) of determining the visited network (N-MNO-B) includes a
20 step of querying a Global Directory (31) about the National Network Operator in charge of assigning a given user's IP address.

19. The method of claim 10, wherein the step d) of receiving a Single Sign-On authentication assertion
25 from the entity where such assertion was generated includes the steps of:

- receiving from the user a reference to said assertion along with an address of such entity; and

- validating the assertion with the entity having
30 generated the assertion.